**La norma ISO 31000:2018**

**Introduzione.**

L’uomo per natura gestisce il rischio in modo consapevole e inconsapevole.

Le decisioni solitamente sono sistematiche ma seguono un approccio: stabilire obiettivi, stimare risultati, confrontarli con gli obiettivi e decidere.

L’incertezza è dovuta alla mancanza della “conoscenza assoluta” della situazione alla quale ci si riferisce, che è un limite invalicabile dell’uomo.

Per affrontare il rischio il normatore ISO (Internation Organization for Standardization) ha emesso delle norme come la **ISO/IEC Guide 73** che fornisce il vocabolario e i termini per il risk management e la **ISO 31000:2018** “Risk management – Guidelines” applicabile ad ogni organizzazione o entità che gestisce i rischi.

La norma ISO 31000 è una linea guida, fornisce indicazioni senza approfondimenti e non può essere usata per audit o certificazioni.

Il risk management potrebbe essere usato su tutta l’organizzazione o su una sola attività/progetto, su tutti i livelli o solo a livello strategico, tattico o operativo.

Il successo della gestione dei rischi dipende dall’efficace gestione del framework, che fornisce la struttura e definisce le risorse necessarie per l’integrazione con i processi dell’organizzazione e da fattori chiave come la definizione del contesto, dal campo di applicazione o dagli stakeholder.

Alcuni benefici del risk management:

* Aumenta la probabilità di soddisfare gli obiettivi
* Aumenta la consapevolezza della necessità di identificare e gestire i rischi.
* Assicura la soddisfazione di requisiti legali e regolamentari
* Migliora la confidenza e fiducia degli stakeholder
* Migliora l’applicazione dei controlli.
* Migliora l’uso delle risorse.
* Migliora la prevenzione degli incidenti.

**Governance**: guida la direzione generale, sia internamente che esternamente.

Definisce regole, processi e pratiche per raggiungere gli obiettivi principali (la missione).

La **gestione strategica** traduce i principi di governance in strategie concrete e obiettivi per garantire risultati sostenibili e soddisfare gli interessi degli stakeholder.

La **risk governance** si occupa di come l'organizzazione identifica, valuta e gestisce i rischi e include la definizione di strategie e le decisioni.

Crea un framework (struttura) per applicare concretamente il processo di gestione dei rischi e coordina i princìpi, il framework e l'implementazione pratica del risk management.

**Il rischio**.

Il rischio in natura non è evitabile, ma può essere ridotto e controllato.

Nella ISO 31000 il rischio è espresso in termini di: fonti di pericolo, potenziali eventi favorevoli o sfavorevoli, le loro conseguenze (danni – o opportunità +) e probabilità.

Con “analisi del rischio” si intende l’individuazione delle possibili cause di un evento e le sue conseguenze.

I rischi si manifestano in caso di **incertezza** che aumenta con la crescita della complessità della situazione 🡪”**Rischio: effetto dell’incertezza sugli obiettivi**.” ISO guide 73.

**Obiettivi**: possono riguardare ambiti diversi (economico, salute…), livelli diversi (strategico, tattico e operativo) ed essere espressi come risultati desiderati, scopo o criterio.

**Effetto**: deviazione rispetto alle aspettative. Positivo o negativo.

**Incertezza**: non conoscenza di un processo, evento o di una entità o situazione. Esiste sempre almeno in parte perché la conoscenza assoluta non esiste. Il rischio dipende dall’incertezza come conoscenza e dall’impatto dell’incertezza.

**Rischio= f(P, D)**: combinazione di probabilità P e impatto D.

La responsabilità per il raggiungimento di un obiettivo e per il controllo della situazione cade sul proprietario dell’obiettivo, che è anche colui che attribuisce valore all’obiettivo e decide la strada per raggiungerlo.

Entità/comportamenti da analizzare: obiettivo, proprietario, fonti di pericolo, vulnerabilità, minacce e controlli.

Esistono sempre Fonti di pericolo che attraverso gli Agenti possono sollevare Minacce ostacolando la soddisfazione degli obiettivi.

L’importanza della soddisfazione dell’obiettivo spinge il proprietario ad applicare Misure (controlli) contro le minacce o le vulnerabilità.

L’organizzazione deve avere un risk-based thinking, cioè, considerare i l rischio parte integrante dei processi e del sistema, per concentrare gli sforzi sui processi chiave e le opportunità di miglioramento aumentando la probabilità di raggiungere gli obiettivi.

**Risk management nel processo decisionale**.

Ogni organizzazione affronta rischi che possono avere impatti sugli obiettivi a livello strategico, tattico o operativo; quindi, deve gestire i rischi che nascono da ogni attività, quel processo si chiama **Risk management**.

Le decisioni si prendono in base alle informazioni a disposizione e la conoscenza non è mai totale.

La natura e il grado di incertezza dipendono dalla qualità, quantità, integrità e provenienza delle informazioni, il metodo di raccolta e elaborazione dati può variare.

La percezione e la consapevolezza sono elementi essenziali per il processo decisionale, mancanza di consapevolezza e scarsa applicazione di pratiche riducono l’efficacia dei processi.

Il livello di **accettabilità** dei rischi evolve con le condizioni sociali, etiche e economiche della collettività, spesso l’evoluzione non è positiva perché comporta nuovi rischi (es: tecnologia).

Benefici del risk management: miglioramento del governo dell’organizzazione, aumento della fiducia degli stakeholder, aumento della solidità dell’organizzazione e del processo decisionale, soddisfazione degli obiettivi prestabiliti, identificazione dei rischi e delle vulnerabilità migliore e conformità alle leggi.

**Principi che guidano il risk management**

Un’organizzazione per avere successo dovrebbe essere gestita attraverso la risk governance in modo sistematico e trasparente.

Il risk management:

* Non è indipendente o separato dai processi e dalle attività dell’organizzazione.
* Gestisce ambienti organizzativi complessi e prende decisioni in situazioni difficili. Il processo decisionale è la somma qualitativa delle singole decisioni strategiche, operative e tattiche.
* Considera le incertezze, la loro natura e la loro causa.
* Deve essere personalizzato per allinearlo al contesto.
* Deve riconoscere capacità, percezioni e intenzioni delle persone che possono facilitare o ostacolare il conseguimento degli obiettivi.
* Sente e risponde al cambiamento (dinamico).
* Deve migliorare continuamente con idoneità, adeguatezza e efficacia del processo.

**Framework per il risk management.**

Il framework (infrastruttura) è l’impostazione che permette di integrare efficacemente il processo di risk manager nel sistema di gestione aziendale.

L’impostazione del framework dovrebbe seguire l’approccio plan-do-check-act che consiste nel progettare, implementare, riesaminare e migliorare il framework.

Componenti del framework:

* Leadership e impegno: necessari per assicurare l’efficacia e efficienza del processo di risk management. Compiti della direzione:
  + Policy: stabilirla, approvarla, assicurarne la compatibilità con la direzione strategica e con la cultura.
  + Assegnare: ruoli, responsabilità, autorità…
  + Mettere a disposizione le risorse adeguate.
  + Assicurare la soddisfazione dei requisiti e l’adeguatezza del framework.
  + Dare supporto ai ruoli di responsabilità.
  + **Definire criteri e livelli di accettazione dei rischi**
  + **Condurre riesami periodici per idoneità, adeguatezza, efficacia ed efficienza.**
  + **Promuovere il miglioramento continuo**.

L’impegno dovrebbe essere appropriato agli scopi, assicurare collegamento tra obiettivi e politiche, stabilire le responsabilità, mettere a disposizione le risorse, contenere l’impegno per mettere a disposizione le risorse e le modalità per misurare le prestazioni.

L’alta direzione dovrebbe assicurare anche le responsabilità, le autorità e le competenze necessarie attraverso l’identificazione di proprietari dei rischi, responsabili per il risk management, stabilendo le responsabilità e garantendo adeguati livelli di riconoscimento.

Il personale dovrebbe possedere la competenza necessaria.

L’organizzazione dovrebbe determinare i canali di comunicazione e reporting e implementare un piano per stabilire cosa/quando/chi/con chi/come comunicare.

* Integrazione
* Progettazione
* Implementazione: definendo una strategia, applicando la politica di gestione rischi, pianificare ed erogare formazioni, mantenendo le competenze e consultando gli stakeholder.
* Valutazione
* Miglioramento

Il risk management dovrebbe essere integrato e vincolato in tutti i processi e in tutte le attività per essere pertinente, efficace ed efficiente. Bisogna determinare il contesto interno ed esterno che va monitorato costantemente perché cambia di continuo.

Immagine che contiene testo, schermata, Parallelo, linea

Descrizione generata automaticamente**Il processo del risk management.**

Composto da diverse fasi:

1. Comunicazione e consultazione.
2. Campo di applicazione, contesto e criteri.
3. Risk assessment: identificazione, analisi e valutazione rischi.
4. Trattamento dei rischi: selezionare le opzioni, identificare misure da implementare ed esistenti, calcolare rischio residuo e preparare il piano.
5. Accettare i rischi.
6. Implementare le misure.
7. Monitoraggio e riesame.
8. Registrazione e reporting.

Il risk management viene eseguito attraverso istanze, cioè applicazioni del processo per un determinato evento o favore di rischio.

La comunicazione e consultazione devono essere svolte in modo continuo per tutto il processo.

Bisogna personalizzare il risk management per rendere efficace il risk assessment e il risk treatment, quindi bisogna stabile: campo di applicazione, contesto interno ed esterno e criteri per la gestione dei rischi.

Contesto esterno: situazione economica/finanziaria, mercato, clienti, concorrenti, ambiente fisico e culturale, tecnologia, alleanze, regolamenti, stakeholder, vicini…

Contesto interno: governance (struttura organizzativa), politiche, obiettivi (e strategie per raggiungerli), risorse, competenze, conoscenze, rapporti con stakeholder, cultura, sistemi informativi, norme e contratti.

Campo di applicazione: confini del contesto di applicazione, esigenze/aspettative degli stakeholder, processi, attività, progetti, ruoli, responsabilità, autorità, risorse, decisioni…

Rischio: R=f(P,D), è legato alla probabilità P (frequenza) e alla severità delle conseguenze D.

Due approcci per il risk assessment: analitico ed empirico.

Analitico: il rischio è associato ad un fattore di rischio (minaccia) che esplora una vulnerabilità.

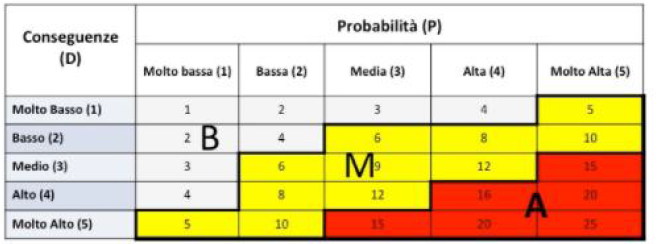
Minaccia + vulnerabilità = evento negativo. Situazione favorevole + opportunità = evento positivo.

Empirico: utilizza matrici di rischio o di probabilità 🡪facili da utilizzare 🡪+ utilizzati.

Criteri per la gestione dei rischi: valori, obiettivi e risorse dell’organizzazione, possono essere imposti o derivati dalle leggi e dovrebbero essere coerenti con la politica.

Fattori: natura/cause/conseguenze degli eventi, livelli di verosimiglianza, misurazione di probabilità e conseguenze (magnitudo), punti di vista degli stakeholder, combinazione dei rischi parziali…

Scala qualitativa delle conseguenze: molto alto (5)>alto (4)>medio (3)>basso (2)>molto basso (1), si crea una scala anche delle probabilità e unendole si forma una matrice.

I tre colori (bianco, giallo e rosso) rappresentano i livelli di accettazione dei rischi: **rischio residuo accettabile RRac** < rischio da ridurre < rischio da ridurre immediatamente.

Identificazione dei rischi: generare una lista dei fattori di rischio basati sugli eventi che potrebbero compromettere o facilitare la soddisfazione degli obiettivi. Prende in considerazione anche fonti, fattori e agenti esterni.

Bow-tie fumatore:

Immagine che contiene testo, schermata, diagramma

Descrizione generata automaticamente

**Analisi dei rischi**: attività attraverso la quale, sulla base di una situazione, si valutano le probabilità degli eventi e le conseguenze sugli obiettivi. Si organizzano tutte le potenziali vulnerabilità e minacce di tipo fisico-ambientale, organizzativo e logico.

Una vulnerabilità può essere sfruttata da una seconda minaccia portando ad un secondo incidente 🡪**Rischio parziale** 🡪entità bassa (1-4) tollerabili.

Anche una minaccia potrebbe sfruttare più vulnerabilità creando più rischi parziali.

**Rischio aggregato**: combinazione dei rischi parziali, posso combinarli con:

Immagine che contiene testo, Carattere, bianco, numero

Descrizione generata automaticamenteImmagine che contiene testo, Carattere, bianco, calligrafia

Descrizione generata automaticamenteMedia ponderata/pesata. Media normale (tutti lo stesso peso).

Ci sono anche altre formule utilizzabili.

Il livello di confidenza dipende dall’approfondimento e dalla conoscenza che si ha sulla situazione reale, per questo si coinvolgono esperti e si svolge l’analisi delle fonti.

Il rischio aggregato dà solo un’indicazione sui rischi e aiuta a decidere le opzioni da seguire, ma non a ridurre o eliminare i rischi.

**Punto decisionale 1**: valutazione dei risultati del Risk Assessment tramite riesame dei risultati della fase precedente. Gli stakeholder devono dare l’approvazione per procedere con il trattamento.

**Trattamento dei rischi**: selezione delle opzioni, identificazione delle misure da implementare o esistenti, calcolo dei rischi residui e preparazione del piano di trattamento dei rischi.

Consiste nella scelta di una delle azioni: modificare, accettare, evitare o condividere i rischi, scegliendo le opzioni che con il minimo sforzo garantiscono il massimo beneficio.

Esistono molti vincoli tecnici che possono ostacolare l’uso di alcune misure o indurre ad errori umani annullando la misura.

Risultato: elenco di possibili misure con costi, benefici e priorità di implementazione.

Condividere i rischi: trasferire i rischi ad altre persone tramite assicurazioni o accordi, non si possono condividere le responsabilità di un impatto.

Immagine che contiene testo, linea, Diagramma, diagramma

Descrizione generata automaticamente**Rischio gestito Rg**: gli amministratori introducono misure inadeguate ai livelli di protezione richiesti ma che possono gestire un certo quantitativo di rischio 🡪calcolo del rischio residuo.

Rischio residuo > Rischio residuo accettabile = bisogna applicare altre misure per ridurre i rischi.

Il Rischio Residuo Accettabile RRac non è statico ma muta così come le minacce, vulnerabilità e le esigenze degli stakeholder ed è la soglia minima al di sopra della quale il rischio deve essere ridotto. Si dà priorità ai rischi “rossi” che non possono essere dilazionati, mentre quelli “gialli” possono essere programmati nel medio/lungo periodo.

Il Piano di Trattamento dei Rischi contiene le informazioni:

* Motivi per la scelta delle opzioni di trattamento ed i benefici attesi.
* Elenco delle misure da implementare (con le priorità) e di quelle già esistenti.
* Calcolo dei rischi residui.
* I responsabili per l’approvazione e attuazione del piano.
* Le competenze necessarie e il training per soddisfare le esigenze.
* Le risorse necessarie per l’implementazione delle misure.
* Le modalità per misurare l’efficacia delle misure.
* Le modalità di registrazione.

I rischi residui devono essere documentati e sottoposti a monitoraggio e riesame.

**Punto decisionale 2:** gestita dal proprietario dei rischi (e degli obiettivi).

Il proprietario rivede e approva le misure proposte e i conseguenti Rischi Residui registrando le condizioni associate all’approvazione.

L’accettazione dei rischi non è un semplice confronto con la soglia, potremmo accettare un rischio perché i vantaggi sono troppo alti e i costi di implementazione delle misure sono eccessivi, in questo caso però forse bisognerebbe rivedere i criteri di accettazione dei rischi.

Implementazione del punto decisionale 2: approvazione del Piano di Trattamento dei Rischi, approvazione dei Rischi Residui e autorizzazione dell’implementazione delle misure.

Si procede con l’implementazione delle Misure stabilite nel Piano, definendo anche le modalità di misurazione, il training necessario e svolgendo monitoraggio e riesame continui.

**Monitoraggio e riesame** permettono di: esaminare l’efficacia del processo di risk management e migliorarlo, apprendere da eventi e cambiamenti, valutare le misure, rilevare cambiamenti del contesto e identificare rischi emergenti.

Attività di monitoraggio e riesame: aspetti legali, ambientali, concorrenziali, risk assessment, riesame degli obiettivi, criteri di valutazione/accettazione rischi, costi di implementazione e competenze richieste.

Le attività del risk management dovrebbero essere tracciabili attraverso **registrazioni**, cartacee o elettroniche e su un qualsiasi supporto, costituendo le fondamenta di efficacia, efficienza e miglioramento continuo del risk management.

Le registrazioni devono essere controllate e conservate e devono tenere conto di: esigenze di apprendimento continuo, benefici del riutilizzo di informazioni a fini di gestione, costi e sforzi di mantenimento delle registrazioni, requisiti legali/normativi, metodo di accesso, periodo di conservazione e sensibilità delle informazioni.

Ogni applicazione del processo dovrebbe produrre informazioni relative a:

* Obiettivi da raggiungere e proprietari degli obiettivi.
* Contesto interno ed esterno dell’istanza, campo di applicazione, estensione dei confini, attività degli stakeholder…
* Ruoli, responsabilità e autorità.
* Proprietà dei rischi e criteri della loro gestione.
* Risk assessment.
* Attività del punto decisionale 1.
* Trattamento dei rischi mediante Piano o accettazione dei rischi (punto decisionale 2).
* Implementazione delle misure e valutazione della loro efficacia.

**Caso di studio: il tesoretto.**

Famiglia: il capofamiglia (proprietario) conserva un tesoretto di 40.000€ nell’appartamento.

Obiettivo: conservare il tesoretto integro.

Contesto esterno: l’appartamento si trova nella periferia nord di una città settentrionale, al primo piano di una palazzina da 8 appartamenti.

La famiglia al piano terra (appartamento 2) ha due figli di cui il maggiore ha precedenti penali.

Portatori di interesse esterni: negozi che vorrebbero avere il capofamiglia come cliente.

Potenziali minacce esterne: malviventi della zona e il figlio dell’appartamento 2.

Contesto interno (stakeholder): nucleo familiare di capofamiglia, moglie e figlio ventiduenne, i genitori lavorano ma il figlio no. 🡪unici a conoscenza del tesoretto.

Immagino: tesoretto in un cassetto senza lucchetto in una stanza con finestra.

Scala di impatto: 1)Molto basso: 10k€ < 2)Basso: 20k€ < 3)Medio: 30k€ < 4)Alto: 40k€ < 5)M. alto 50k€.

Scala probabilità: 1)Molto basso < 2)Basso < 3)Medio < 4)Alto < 5)Molto alto.

Si potrebbe analizzare la situazione con tecniche di brainstorming, check-list o interviste.

Vulnerabilità:

1. V1: Porta del salone in cui è custodito il tesoretto.
2. V2: Porta d’ingresso dell’appartamento
3. V3: Finestra del salone affacciata sull’esterno.

Poi bisognerebbe fare un’analisi per vedere se ci sono agenti portatori di minacce come ladri che vogliono impossessarsi del tesoretto, ma anche agenti meno evidenti come umidità o incendi.

Minaccia M1: figlio del capofamiglia disoccupato 🡪 prelievo del tesoretto totale o parziale (75% - 30.000€) 🡪v1.

Minaccia M2: famiglia al primo piano che viene a conoscenza del tesoretto 🡪furto totale (D=40.000€) e uso di V2 o V3.

Combinazioni: (M1, V1)🡪D13=30k€ o (M2, V2) o (M2, V3)🡪D4=40k€.

Probabilità: P1\_1(M1, V1)=5, P2\_2(M2,V2)=4, P2\_3(M2,V3)=3.

Rischi parziali:

R1=f(P1\_1,D1)=5\*3=15; R2=f(P2\_2,D2)=4\*4=16; R3=f(P2\_3,D2)=3\*4=12.

**Rischio aggregato** tramite media aritmetica: 15+16+12=43/3=14 🡪rischio complessivo medio.

Il capofamiglia decide se intervenire spostando il tesoretto (cambiando tuti i rischi) o di lasciarlo lì e lavorare sui singoli rischi parziali che lo compongono.

Operazioni possibili: modificare, accettare, evitare o condividere/trasferire i rischi.

Evitare i rischi (trasferirli): portarli in banca. Modificare i rischi: introdurre misure adeguate.

Accettare i rischi non è percorribile (livello medio di Ragg e Medio/Alto di Rp).

Ridurre i rischi parziali:

1. Immagine che contiene testo, schermata, numero, Carattere

   Descrizione generata automaticamenteR1: figlio: rimuovere la vulnerabilità (serratura alla porta o cassaforte) o allontanare la minaccia spingendolo a trovarsi un lavoro. Misure: c1 (lavoro), C2 (cassaforte), C3 (porta del salone chiusa a chiave), C4 (sensibilizzare il figlio).
2. R2: malviventi attraverso la porta: C2 (cassaforte), C5 (porta blindata all’ingresso).
3. R3: malviventi dalla finestra: C2 (cassaforte), C6 (finestra).

C5 (porta blindata) è già implementata 🡪riduce valore di R2 di quantità R2\_g2c5.

Rischio residuo parziale R1: R1=15, se applico tutte le misure (C1, C2, C3, C4) scende da liv 15 a liv 1.

RR1=R1-RG1=15-14=1.

Rischio residuo parziale R2: R2=16, applicando C2 e C5 scende a 1. RR2=R2-RG2=16-15=1.

Rischio residuo parziale R3: R3=12, applicando C2 e C6 scende a 1. RR3=R3-RG3=12-11=1.

🡺Rischio residuo aggregato: RRaggr=1.

Il proprietario approva il Piano di Trattamento Rischi e approva i Rischi Parziali Residui: RR1=1, RR2=1, RR3=1, RRaggr=1. Tutti i rischi parziali residui RRi sono sotto il livello di accettazione.

In seguito, il proprietario deve approvare i RRi e procedere implementando le contromisure stabilite nel piano provvedendo all’investimento delle competenze, alle risorse e ad ogni altro supporto.

**Caso di studio: passaggio a livello.**

Premessa: in questo caso, per la natura della situazione, non è possibile seguire in modo rigoroso il processo del risk management 🡪 impossibile raccogliere dati o compiere analisi.

Le uniche analisi sono qualitative basate sui ragionamenti del momento (soggettive).

**Evento**: un uomo deve andare in ufficio a piedi impugnando una borsa con documenti e laptop.

Deve arrivare puntuale (almeno 15 min prima) 🡪Passaggio a livello chiuso.

**Obiettivo**: attraversare il passaggio a livello per arrivare in orario e non essere investito.

Creiamo delle scale di probabilità e di conseguenze da 1 a 5 e ordiniamo le azioni per priorità crescente di rischio (priorità = rischio basso).

Il **contesto** offre le seguenti opzioni:

1. Attraversare comunque i binari 🡪rischio di essere investito
2. Usufruire del ponte sopraelevato 🡪+400m di strada, pioggia e borsa in mano 🡪rischio di farsi male e ritardo 15-30 min.
3. Cambiare strada allungando il percorso 🡪ritardo 15-30 min.
4. Aspettare che passino tutti i treni e si alzino le sbarre 🡪ritardo >30 min.

R1: rischio = essere investito dal treno🡪D=5 \* P=5 🡪R=25.

R2: farsi male sul ponte di ferro 🡪 P=4 \* D=5 🡪R=20.

R3: ritardo cambiando strada 🡪 P=3 \* D=1 🡪R=3.

R4: ritardo per aspettare il passaggio a livello 🡪P=5 \* D=1 🡪R=5. (Io metterei D=2).

Le scelte migliori sono R3 e R4 🡪meglio R3 perché il ritardo di D4 è meno prevedibile.

Una volta deciso il da farsi: chiamare il collega per avvisare del ritardo, tracciare il nuovo percorso e avviarsi attraverso esso.

Monitoraggio continuo: controllare il tempo ed il percorso mentre si cammina avvisando in ufficio per ulteriori ritardi.

Per migliorare la situazione per le prossime volte: partire prima (soprattutto se piove), informarsi sugli orari di chiusura del passaggio a livello, chiedere di non pianificare le riunioni importanti al mattino presto e considerare la possibilità di una riunione con collegamento da remoto.

**Caso di studio: la mensa scolastica.**

**Introduzione**: la mensa scolastica viene fornita da aziende specializzate o dalla scuola, è situata all’interno dell’edificio ma in un’area dedicata e separata.

Sono aperte durante gli orari dei pasti e offrono pasti fissi gratuiti o a pagamento.

Devono stare a standard qualitativi e possono avere supervisione.

Risk management event-based gestito da un gruppo con: 1 responsabile, 3 genitori, 4 studenti, 1 persona dell’amministrazione, 2 insegnanti e un bidello.

Contesto esterno:

* Area urbana residenziale🡪possibile ritardo dei fornitori.
* Budget 🡪qualità del pasto.
* Cultura alimentare
* Legislazione locale e nazionale 🡪norme della mensa.

Contesto interno: ambiente fisico.

* Disposizione dei tavoli: 2 file per ottimizzare lo spazio e facilitare passaggio.
* Disposizione del cibo: buffet a scelta, cibo più gettonato facilmente accessibile.
* Gestione degli studenti: prenota al mattino e serviti in ordine di arrivo 🡪meno tempo di attesa.
* Pulizia e igiene: 2 operatori.
* Medico nutrizionista che fa la dieta.

Processi:

* Gestione degli ordini: raccolta ordini e calendario consegne.
* Gestione forniture: magazzino e acquisto materie prime.
* Preparazione pasti: cucina, controllo qualità e servizio tavoli.
* Gestione rifiuti: raccolta e smaltimento.
* Gestione attività amministrative: contabilità, risorse umane…
* Gestione reclami e segnalazioni utenti.
* Valutazione dei servizi.

Analisi delle esigenze e aspettative: la valutazione dei rischi in una mensa deve essere fatta regolarmente per garantire la sicurezza degli alimenti e dovrebbe coinvolgere utenti, genitori, scuola, fornitori, dipartimento sanitario, autorità locali…

Aspettative: cibo sano e nutriente, varie opzioni di menu, ambiente pulito, servizio rapido e efficiente, soluzioni dietetiche, partecipazione degli studenti, rispetto per culture e religioni.

Reclami: prezzi e opzioni di pagamento.

Probabilità e impatti vengono divisi in 5 livelli.

**Risk assessment**: brainstorming di rischi/opportunità del contesto interno.

Si considerano le coppie di impatto-probabilità e si confrontano con i criteri di accettazione dei rischi dividendo i fattori di rischio in quelli da mitigare immediatamente, da mitigare e da ignorare.

Sono stati stabiliti i controlli da adottare tramite brainstorming.

Es:

Aspetto: pulizia e igiene 🡪Fattore di rischio: non vengono curate 🡪priorità: alta 🡪controlli: sistema di controllo efficace per le pulizie. Controlli esistenti: sì.

Aspetto: gestione rifiuti 🡪Fattore di rischio: studenti non la seguono 🡪priorità: alta 🡪controlli: posizionare in modo chiaro i bidoni e etichettarli. Controlli esistenti: no.

I controlli riducono il rischio di una certa quantità 🡪 rischio residuo=rischio – rischio gestito.

**Caso di studio: Network Attached Storage**

Molte aziende utilizzano data storage per conservare grandi volumi di dati, possono essere magnetici, ottici o semiconduttori.

La tecnologia comprende: dispositivi, oggetti e processi per memorizzare i dati in modo durevole ed è divisa in base all’ubicazione (collegato direttamente allo storage DAS o tramite rete) e in base all’archiviazione (su blocchi, su file o su oggetti).

**DAS**: il dispositivo di archiviazione può far parte del pc (collegato al Bus) o esterno (USB).

**Archiviazione di rete**: classificata in base al tipo di accessi e archiviazione tra cui il NAS a livello file e SAN a livello blocco.

Prendiamo in considerazione una PMI composta da una LAN bus 🡪rottura in un qualsiasi punto del cavo causa interruzione del servizio 🡪devo preservare le R-I-D.

**Contesto esterno**: periferia tranquilla non solo industriale, cortile recintato, azienda in mezzo al bosco con un fiume vicino. LAN connessa a internet tramite rooter e FW.

**Contesto interno**:

Sistema informatico: LAN bus + 2 desktop pc + workstation con stampante A4, 8 portatili, 8 smartphone, uno switch, un NAS, una stampante in rete, un rooter e un FW.

**Sicurezza fisica e ambientale**:

* Muri perimetrali in cortile + porta videosorvegliata
* Ingresso con chiavi distribuite ma elencate e con firma di accettazione chiave.
* Ingresso agli uffici unico e controllato, ospiti solo accompagnati ma non registrati.

**Asset**: registro asset inventory: apparecchiature elettroniche (critico) manutenzione ordinaria e straordinaria dal responsabile. 🡪asset-based approach.

**Parti interessate**: direzione, clienti e fornitori (e loro dipendenti) e dipendenti della ditta.

Si creano scale per probabilità e impatto su 5 livelli. Rischio accettabile= liv basso (1-4).

Conseguenze: gli utenti che hanno accesso al NAS hanno privilegi di tipo CRUD.

Immagine che contiene testo, numero, Carattere, parole crociate

Descrizione generata automaticamentePer il rischio aggregato si usa la media aritmetica.

Immagine che contiene testo, numero, Carattere

Descrizione generata automaticamente

Punto decisionale 1: i rischi parziali devono essere mitigati secondo la priorità per renderli accettabili 🡪si modificano o eliminano i rischi e si calcolano i controlli già presenti e quelli da aggiungere.

Rischio residuo = rischio parziale – rischio gestito.

Punto decisionale 2: approvazione del piano di trattamento rischi e accetta i rischi parziali.

**Caso di studio: perdita di personale chiave.**

Azienda che sviluppa app web e siti internet, l’azienda fornisce servizi di sviluppo sw tra cui: sviluppo sw ad hoc, realizzazione di componenti di sw, integrazione e ottimizzazione dei sw in uso e delle pagine web e organizzazione dei contenuti in modo che il risultato sia un sito web visibile, dinamico e facile da aggiornare. Asset: perdita di personale chiave🡪event-based approach.

Contesto: perdita di personale chiave🡪 + doppio del suo stipendio.

Contesto esterno: mercato delle figure professionali con competenze digitali, elevata concorrenza per attrarre talenti e l’offerta di persone non copre la domanda.

Contesto interno: creazione di un clima lavorativo positivo per mantenere i dipendenti: incoraggia la creatività, rende partecipe i dipendenti del successo dell’azienda, ambiente di lavoro sicuro, riconosce i risultati individuali.

Conseguenze e probabilità in una scala 1-5.

Immagine che contiene testo, numero, documento, Carattere

Descrizione generata automaticamente**Asset**: personale chiave. **Evento sfavorevole**: perdita di personale chiave. Utilizzano il bow-tie.

Poi si crea la mappa dei rischi bianco-gialla-rossa e si forma un gruppo per selezionare le opzioni per il trattamento dei rischi: Responsabile risorse umane, Responsabile operations e un esperto che fanno brainstorming e bow-tie per identificare i controlli.

Rischio residuo= rischio parziale – rischio gestito.